No title availabl .

Patent Number:	DE19600556
Publication date:	1997-07-24
Inventor(s):	GRASSMANN NORBERT (DE)
Applicant(s)::	SIEMENS AG (DE)
Requested Patent:	☐ DE19600556
Application Number:	DE19961000556 19960109
Priority Number(s):	DE19961000556 19960109
IPC Classification:	E05B49/00 ; B60R25/00 ; B60R25/04 ; G07C9/00
EC Classification:	E05B49/00J6F, G08C19/28
Equivalents:	BR9700026, ☐ FR2743386, ☐ GB2309046

Abstract

A lock (1) (eg for a motor vehicle) sends a random number to a key (2), which applies a crypto algorithm to the random number and sends a code word back to the lock (1). In the lock (1), the code word is compared with a desired code word, which is generated by applying the same crypto algorithm to the random number. An authentication signal is then generated so long as the code word and the desired code word are substantially but not necessarily completely in agreement.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) Offenlegungsschrift

(10) DE 196 00 556 A1

(51) Int. Cl.[6]:
E 05 B 49/00
B 60 R 25/00
B 60 R 25/04
G 07 C 9/00

(21) Aktenzeichen: 196 00 556.6
(22) Anmeldetag: 9. 1. 96
(43) Offenlegungstag: 24. 7. 97

DE 196 00 556 A1

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Grassmann, Norbert, 93057 Regensburg, DE

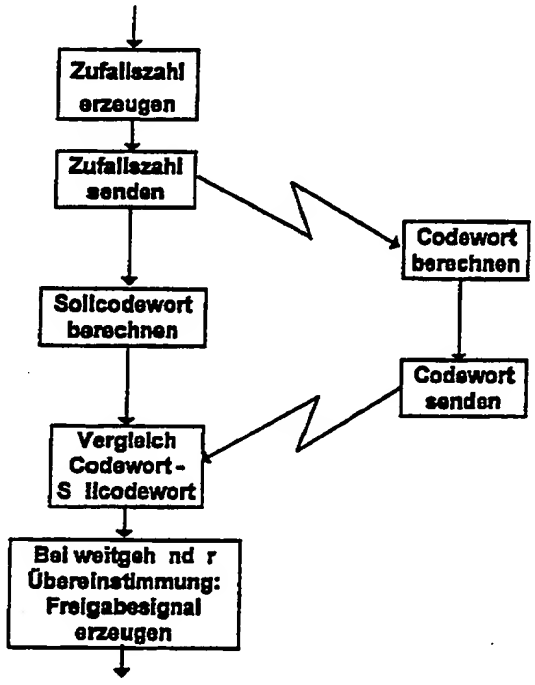
(56) Entgegenhaltungen:

DE	44 01 852 C1
DE	32 25 754 A1
EP	06 83 293 A1
EP	04 92 692 A2

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Betreiben eines Diebstahlschutzsystems und Diebstahlschutzsystem

(57) Ein Schloß (1) sendet eine Zufallszahl zu einem Schlüssel (2). Der Schlüssel (2) wendet einen Kryptoalgorithmus auf die Zufallszahl an und sendet ein Codewort zurück zum Schloß (1). Im Schloß (1) wird das Codewort mit einem Sollcodewort verglichen, das durch Anwenden des gleichen Kryptoralgorithmus auf die Zufallszahl erzeugt wird. Ein Freigabesignal wird erfindungsgemäß bereits dann erzeugt, wenn nicht alle, aber ein Großteil der Bits des Sollcodeworts und ein Großteil des empfangenen Codeworts übereinstimmen.



DE 196 00 556 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Beschreibung

Die Erfindung betrifft ein Verfahren zum Betreiben eines Diebstahlschutzsystems, insbesondere für ein Kraftfahrzeug, und ein Diebstahlschutzsystem.

Ein bekanntes Diebstahlschutzsystem (EP 0 257 376 A1) weist einen Schlüssel und ein Schloß auf. Der Schlüssel sendet bei Betätigen ein Codesignal aus, das im Schloß mit einem Sollcodesignal verglichen wird. Wenn das Codesignal nicht mit dem Sollcodesignal übereinstimmt, wird innerhalb eines ersten Fangbereichs nachgeschaut, ob dort ein gleiches Sollcodesignal vorhanden ist. Wenn auch in dem ersten Fangbereich keine Übereinstimmung besteht, so müssen zwei aufeinanderfolgende Codesignale mit zwei aufeinanderfolgenden Sollcodesignalen übereinstimmen.

Bei diesem Diebstahlschutzsystem muß eine vollständige Übereinstimmung zwischen dem übertragenen Codesignal und dem im Schloß errechneten Sollcodesignal bestehen. Bei Übertragungsstörungen, die das Codesignal zum Teil verfälschen, können entweder die Türen nicht entriegelt werden oder es muß ein erneuter Versuch gestartet werden.

Der Erfindung liegt das Problem zugrunde, ein Diebstahlschutzsystem zu schaffen, das ein sicheres Ver- oder Entriegeln oder ein sicheres Lösen der Wegfahrsperre auch bei Übertragungsstörungen zuläßt.

Dieses Problem wird erfindungsgemäß durch ein Verfahren mit den Merkmalen von Patentanspruch 1 und durch ein Diebstahlschutzsystem mit den Merkmalen von Anspruch 5 gelöst.

Vorteilhafte Ausgestaltung der Erfindung sind in den Unteransprüchen gekennzeichnet.

Ein Ausführungsbeispiel der Erfindung wird im folgenden anhand der schematischen Zeichnungen näher erläutert. Es zeigen:

Fig. 1 Ein schematisches Blockschaltbild des erfindungsgemäßen Diebstahlschutzsystems,

Fig. 2 Codeworte des Diebstahlschutzsystems und

Fig. 3 Ein Ablaufdiagramm eines Verfahrens zum Betreiben des Diebstahlschutzsystems.

Ein erfindungsgemäßes Diebstahlschutzsystem weist ein Schloß 1 (**Fig.** 1) und einen Schlüssel 2 auf. Im Schloß 1 ist eine Recheneinheit 11 angeordnet, die zunächst eine Zufallszahl erzeugt (vgl. auch **Fig.** 3). Die Zufallszahl wird mit Hilfe einer Sende- und Empfangseinheit, die einen Schwingkreis mit einer Spule 12 und einem Kondensator 13 aufweist, zum Schlüssel 2 übertragen, wenn der Schlüssel 2 in unmittelbarer Nähe des Schlosses 1 angeordnet ist.

Im Schlüssel 2 ist ebenfalls ein Sende- und Empfangseinheit mit einem Schwingkreis, der eine Spule 21 und einen Kondensator 22 aufweist, über die die Zufallszahl empfangen wird. Die Zufallszahl wird einer schlüsselseitigen Recheneinheit 23 zugeführt, die einen mathematischen Algorithmus auf die Zufallszahl und auf eine in dem Schlüssel 2 gespeicherte, nicht auslesbare Geheimzahl mehrfach anwendet.

Somit wird ein Codewort erzeugt, das über die induktiv miteinander gekoppelten Spulen 12, 21 zu dem Schloß 1 zurückübertragen wird.

In der Recheneinheit 11 des Schlosses 1 wird der gleiche mathematischen Algorithmus wie im Schlüssel 2 auf die Zufallszahl und die ebenfalls im Schloß 1 gespeicherte Geheimzahl angewendet. Somit wird im Schloß 1 ein Sollcodewort erzeugt, das einem Komparator 14 zugeführt wird. Das von dem Schlüssel 2 empfangene Codewort wird dem Komparator 14 ebenfalls zugeführt. Das Codewort und das Sollcodewort werden in dem Komparator 14 miteinander verglichen und wenn zumindest in Großteil des Codeworts und ein Großteil des Sollcodeworts miteinander übereinstimmen, wird ein Freigabesignal erzeugt, das die Türen des Fahrzeugs ver- oder entriegelt oder die Wegfahrsperre löst.

Die Codeworte und die Zufallszahl sowie die Geheimzahl sind binär codierte Signale mit jeweils einer vorgegebenen Anzahl von Bits. So kann beispielsweise die Zufallszahl 6 Byte, d. h. 48 Bit lang sein. In dem Schlüssel 2 kann eine Geheimzahl mit einer Länge von 16 Byte gespeichert sein. Als einfachstes Beispiel eines mathematischen Algorithmus kann beispielsweise eine EXOR-Verknüpfung auf die Zufallszahl und die Geheimzahl mehrfach angewendet werden, so daß z. B. ein 6 Byte langes Codewort erzeugt wird. Das gleiche geschieht im Schloß 1, wo ein 6 Byte langes Sollcodewort aus der Zufallszahl sowie der Geheimzahl und dem mathematischen Algorithmus erzeugt wird.

Das empfangene Codewort und das erzeugte Sollcodewort werden in dem Komparator Bit für Bit miteinander verglichen. Infolge von Übertragungsstörungen, die durch EMV-Störungen in der Umgebung des Diebstahlschutzsystems oder durch externe Störsender verursacht sind, kann es vorkommen, daß die Übertragung des Codeworts gestört wird. Dadurch können sich einige Bits des Codeworts unbeabsichtigt verändern. Die Auswirkungen einer solchen Störung sind beispielhaft in der **Fig.** 2 dargestellt. Dort ist das Codewort oben dargestellt und unterscheidet sich infolge einer Störung in zwei Bits von dem unten dargestellten Sollcodewort.

Bei dem erfindungsgemäßen Diebstahlschutzsystem ist es nun zugelassen, daß sich das empfangene Codewort und das erzeugte Sollcodewort in einer vorgegebenen maximalen Anzahl von fehlerhaften Bits, zum Beispiel von 10 Bits, unterscheiden. Erst wenn sich die beiden Codeworte um mehr als die maximale Anzahl von fehlerhaften Bits unterscheiden, wird das Freigabesignal nicht mehr erzeugt.

Das Diebstahlschutzsystem kann auch derart ausgestaltet sein, daß pro Byte (d. h. pro 8 Bit) oder pro 4 Bit ein einziges fehlerhaftes Bit zugelassen wird. In diesem Fall würde ein Codewort nach **Fig.** 2 nicht zu einem Freigabesignal führen, da im zweiten Byte gleich zwei Bits fehlerhaft sind. Je weniger fehlerhafte Bits insgesamt zugelassen werden, desto höher ist die Sicherheit des Diebstahlschutzsystems. Aber gleichzeitig steigt die Anfälligkeit gegen äußere Störungen.

Mit diesem Diebstahlschutzsystem wird erreicht, daß die Wegfahrsperre beim Starten des Kraftfahrzeugs auch bei kleineren EMV-Störungen gelöst werden kann. Es ist dann kein zweiter Startversuch mehr notwendig. Ebenso können die Türen sicher ent- oder verriegelt werden.

Die Funktion einer Wegfahrsperre kann dabei in einem Motorsteuergerät realisiert sein. Nur wenn das berechtigte Freigabesignal zum Motorsteuergerät gelangt, ist ein Starten des Motors und ein Fahren des Kraftfahrzeugs möglich. Das Motorsteuergerät kann auch die Zufallszahl erzeugen und dem Schloß 1 zuleiten.

Dem Codewort kann auch einen fahrzeugspezifischen Anteil aufweisen, der entweder an das Codewort vor dem Aussenden angehängt wird oder auf den auch der mathematische Algorithmus angewendet wird. Das Sollcodewort muß dann auch einen solchen fahrzeugspezifischen Teil aufweisen.

Die Recheneinheit im Schlüssel 2 und im Schloß 1

kann als Kryptotransponder ausgebildet sein. In einem solchen Transponder läuft ein festgelegter mathematischer Algorithmus ab, der auf die Zufallszahl und die Geheimzahl mehrfach angewendet wird. Der Algorithmus kann von außen nicht ausgelesen werden.

Die Energie für den Schlüssel 2 kann mit der Zufallszahl zu dem Schlüssel 2 gesendet und in einem Energiespeicher 24 zwischengespeichert werden. Der Schlüssel 2 kann aber auch eine eigene Batterie oder einen wiederaufladbaren Akkumulator aufweisen.

Als Schlüssel 2 wird bei dem Diebstahlschutzsystem eine Vorrichtung bezeichnet, die ein Zufallswort empfängt, dieses verarbeitet und ein Codewort zu dem Schloß 1 zurücksendet. Diese Vorrichtung kann auf einem herkömmlichen mechanischen Schlüssel 2, auf einer scheckkartengroßen Karte oder auf einer funktionell gleichwertigen mechanischen Vorrichtung angeordnet sein.

Als Schloß 1 wird eine Vorrichtung bezeichnet, die das Zufallswort aussendet und das Codewort empfängt. Das empfangene Codewort wird mit einem im Schloß 1 erzeugten Sollcodewort verglichen. Das Schloß 1 erzeugt bei berechtigtem Codewort ein Freigabesignal, das an ein Sicherheitsaggregat, wie die Wegfahrsperre, oder an die Türverriegelungen ausgesendet wird.

Das erfindungsgemäße Verfahren zum Betreiben eines Diebstahlschutzsystems kann überall dort verwendet werden, wo bisher Kryptoverfahren zur Identifikation oder Authentifikation eingesetzt werden. So kann es beispielsweise auch für Krypto-Chipkarten, Telefonkarten, Scheckkarten für den Geldautomaten, usw. eingesetzt werden.

Vorteilhafterweise wird das Diebstahlschutzsystem bei Kraftfahrzeugen verwendet, wobei der Schlüssel 2 ein Zündschlüssel ist, der dann die Zufallszahl empfängt, wenn der Zündschlüssel im Zündschloß steckt und zum Starten des Motors im Zündschloß gedreht wird.

Patentansprüche

1. Verfahren zum Betreiben eines Diebstahlschutzsystems, insbesondere für ein Kraftfahrzeug, mit einem Schloß (1) und einem Schlüssel (2), **gekennzeichnet durch** folgende Schritte:
   - daß ein erstes Codewort im Schloß (1) erzeugt und von einem schloßseitigen Sender (12) zu dem Schlüssel (2) gesendet wird,
   - daß im Schlüssel (2) ein zweites Codewort aus dem ersten Codewort und mit Hilfe eines im Schlüssel gespeicherten mathematischen Algorithmus erzeugt wird,
   - daß das zweite Codewort über einen schlüsselseitigen Sender (21) zu dem Schloß (12) gesendet wird,
   - daß das zweite Codewort einer schloßseitigen Vergleichseinheit (14) zugeleitet wird,
   - daß ein Sollcodewort in einer schloßseitigen Recheneinheit (11) aus dem ersten Codewort und einem mathematischen Algorithmus, der gleich dem Algorithmus im Schlüssel (2) ist, erzeugt und ebenfalls der Vergleichseinheit (14) zugeleitet wird, und
   - daß das empfangene, zweite Codewort in der Vergleichseinheit (14) mit dem Sollcodewort verglichen wird und wenn zumindest ein Teil des Codeworts mit zumindest einem Teil des Sollcodeworts übereinstimmt, ein Freigabesignal erzeugt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der mathematische Algorithmus ein Kryptoalgorithmus ist.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Sollcodewort und das empfangene, zweite Codewort Bit für Bit miteinander verglichen werden und wenn zumindest eine Mindestanzahl von Bits übereinstimmt, das Freigabesignal erzeugt wird.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Sollcodewort und das empfangene, zweite Codewort in Gruppen von jeweils mehreren Bits miteinander verglichen wird und wenn jeweils zumindest alle Bits einer Gruppe bis auf eines mit denjenigen des Sollcodeworts übereinstimmen, das Freigabesignal erzeugt wird.

5. Diebstahlschutzsystem, insbesondere für ein Kraftfahrzeug, mit einem Schlüssel (1) und einem Schloß (2), das mit einem Verfahren nach Anspruch 1 betrieben wird.

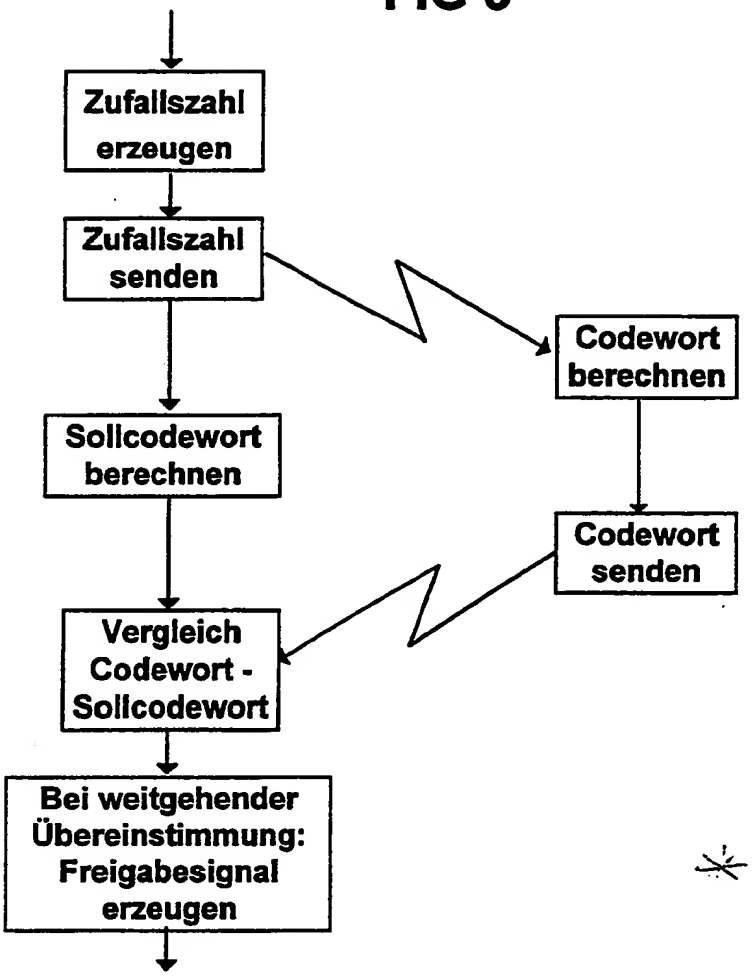
6. Diebstahlschutzsystem nach Anspruch 5, dadurch gekennzeichnet, daß der schloßseitige Sender und der schlüsselseitige Sender als Spulen (12, 21) ausgebildet sind, wobei die Codeworte transformatorisch zwischen den Spulen hin- und her übertragen werden.

Hierzu 2 Seite(n) Zeichnungen

- L rseite -

Nummer: DE 196 00 556 A1
Int. E 05 B 49/00
Offenlegungstag: 24. Juli 1997

FIG 3



Nummer: DE 196 00 556 A1
Int. Cl.: E 05 B 49/00
Offenlegungstag: 24. Juli 1997

FIG 1

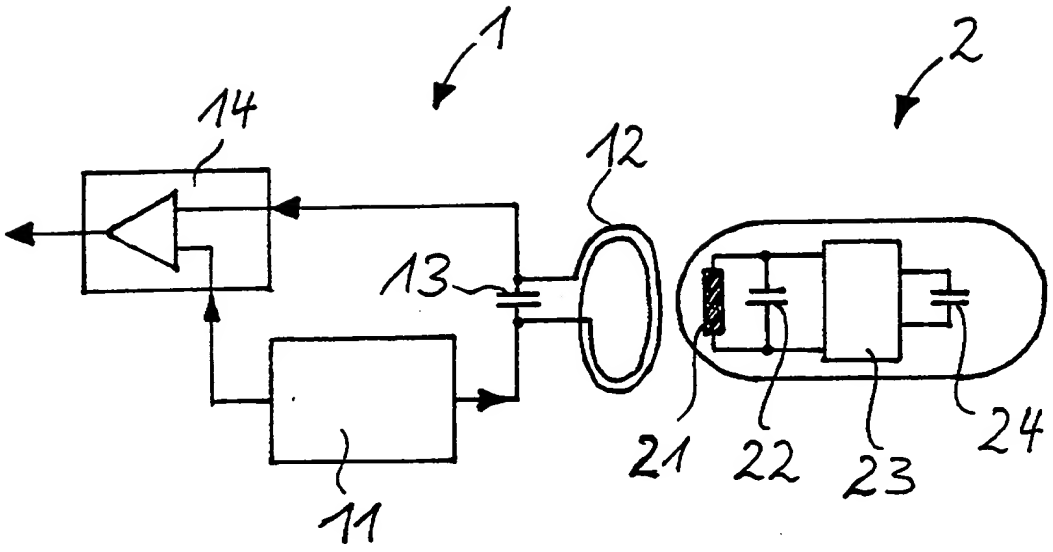


FIG 2